Amendments to the Claims

This listing of claims will replace all prior versions and listings of claims in the application:

Listing of Claims

Claim 1 (Currently amended): A communication system having a server for providing a Web E-mail service to a client, wherein said server comprises:

management means for managing a key for decrypting an encrypted E-mail;

web encryption communication means for establishing a Web encryption communication with the client, and communicating with the client by the established Web encryption communication;

authentication means for executing authentication of the use allowance of the managed key to said client when said client requests to decrypt the encrypted E-mail while said server communicates with the client by said established Web encryption communication;

decrypting means for decrypting the encrypted E-mail using the managed key in the case where the use allowance is authenticated by said authentication means; and

transmission control means for controlling to transmit the E-mail decrypted by said decrypting means to said client through ~~a Web~~ said established Web encryption communication.

Claim 2 (Cancelled)

Claim 3 (Previously presented): The communication system according to claim 1, wherein said authentication means provides said client with a window data to authenticate the use allowance of the managed key.

Claim 4 (Previously presented): The communication system according to claim 1, wherein

said authentication means authenticates the use allowance using a passphrase inputted from said client.

Claim 5 (Previously presented): The communication system according to claim 1, wherein said authentication means authenticates the use allowance based on a biometrics information of a user inputted from said client.

Claim 6 (Currently amended): The communication system according to claim 1, wherein ~~said server further comprises~~ said web encryption communication means ~~for establishing and communicating a Web encryption communication when starting to communicate with said client through the Web~~ establishes the Web encryption communication with the client by using SSL.

Claim 7 (Cancelled).

Claim 8 (Currently amended): The communication system according to claim ~~7~~ 1, wherein said authentication means authenticates the use allowance of the managed key during a session of the Web encryption communication continuously established between said client and ~~a~~ server.

Claim 9 (Previously presented): The communication system according to claim 8, wherein said authentication means stops said authenticated use allowance, in the case where at least either the case where the Web encryption communication is ended with an error or the case where the Web encryption communication has passed a fixed time is satisfied.

Claim 10 (Previously presented): The communication system according to claim 1, wherein said server further comprises signature means for executing a digital signature to an E-mail created by said client.

Claim 11 (Previously presented): The communication system according to claim 1, wherein

said server further comprises:

multiple use judging means for judging whether the managed key is under multiple use, and

stop means for stopping the use allowance of a session under multiple use in the case where the session is judged to be under multiple use by said multiple use judging means.

Claim 12 (Previously presented): The communication system according to claim 1, wherein the key for decrypting the encrypted E-mail is a secret key in a code of a public key cryptosystem.

Claim 13 (Currently amended): A communication system having a client receiving a Web E-mail service from a server, wherein the server comprises:

management means for managing a key for decrypting an encrypted E-mail;

web encryption communication means for establishing a Web encryption communication with the client, and communicating with the client by the established Web encryption communication;

authentication means for executing authentication of the use allowance of the managed key to said client based on authentication information sent from said client when said client requests to decrypt the encrypted E-mail while said server communicates with the client by the established Web encryption communication;

decrypting means for decrypting the encrypted E-mail using the managed key in the case where the use allowance is authenticated by said authentication means; and

transmission control means for controlling to transmit the E-mail decrypted by said decrypting means to said client through ~~a Web~~ the established Web encryption communication, and

wherein said client comprises:

request means for requesting to decrypt the encrypted E-mail while said Web encryption communication is established between the server and the client;

authentication information sending means for sending the authentication information to said authentication means; and

receiving means for receiving the decrypted E-mail transmitted by said transmission control means through ~~the~~ said established Web encryption communication.

Claim 14 (Currently amended): A method for controlling a communication system including a server for providing a client with a Web E-mail service, comprising:

a management step of managing a key for decrypting an encrypted E-mail;

a web encryption communication step for establishing a Web encryption communication with the client, and communicating with the client by the established Web encryption communication;

an authentication step of executing authentication of the use allowance of the managed key to said client when said client requests to decrypt the encrypted email while said server communicates with the client by said established Web encryption communication;

a decrypting step of decrypting the encrypted E-mail using the managed key in the case where the use allowance is authenticated in said authentication step; and

a transmission control step of controlling to transmit the E-mail decrypted in said decrypting step to said client~~, in the server~~ through said established Web encryption communication.

Claim 15 (Cancelled)

Claim 16 (Previously presented): A method for controlling the communication system

according to claim 14, wherein, in said authentication step, a window data for authenticating the use allowance of the managed key is supplied to said client for authentication.

Claim 17 (Previously presented): A method for controlling the communication system according to claim 14, wherein, in said authentication step, the use allowance is authenticated using a passphrase inputted from said client.

Claim 18 (Previously presented): A method for controlling the communication system according to claim 14, wherein, in said authentication step, the use allowance is authenticated based on biometrics information of a user inputted from said client.

Claim 19 (Currently amended): A method for controlling the communication system according to claim 14, wherein, in said server, ~~the method further comprises an~~ said web encryption communication step ~~of establishing and communicating the Web encryption communication when starting to communicate with said client through the Web~~ establishes the Web encryption communication with the client by using SSL.

Claim 20 (Cancelled).

Claim 21 (Currently amended): A method for controlling the communication system according to claim ~~20~~ 14, wherein, in said authentication step, the use allowance of the managed key is authenticated during a session of the Web encryption communication continuously established between said client and ~~a~~ server.

Claim 22 (Previously presented): A method for controlling the communication system according to claim 21, wherein, in said authentication step, said authenticated use allowance is stopped in the case when at least either the case where the Web encryption communication is ended with an error or the case where the Web encryption communication has passed a fixed time is satisfied.

Claim 23 (Previously presented): A method for controlling the communication system according to claim 14, further comprising a signature step of executing the digital signature to the E-mail created by said client in said server.

Claim 24 (Previously presented): A method for controlling the communication system according to claim 14, further comprising a step of executing a multiple use judging step of judging whether the managed key is under multiple use in the server, and a stop step of stopping the use allowance of a session under multiple use in the case where the session is judged to be under multiple use in said multiple use judging step.

Claim 25 (Previously presented): A method for controlling the communication system according to claim 14, wherein the key for decrypting the encrypted E-mail is a secret key in an encryption of a public key cryptosystem.

Claim 26 (Currently amended): A method for controlling a communication system including a client receiving a Web E-mail service from a server, comprising:

a step of executing a management step of managing a key for decrypting an encrypted E-mail,

a web encryption communication step for establishing a Web encryption communication with the client, and communicating with the client by the established Web encryption communication,

an authentication step of executing authentication of the use allowance of the managed key to said client based on authentication information sent from said client when said client requests to decrypt the encrypted E-mail while said server communicates with the client by the established Web encryption communication,

a decrypting step of decrypting the encrypted E-mail using the managed key in the case where the use allowance is authenticated in said authentication step, and

a transmission control step of controlling to transmit the E-mail decrypted in said decrypting step to said client ~~in the server~~ through the established Web encryption communication,

wherein said client comprises:

a requesting step of requesting to decrypt the encrypted E-mail while said Web encryption communication is established between the server and the client,

an authentication information sending step of sending the authentication information for authentication in said authentication step, and

a receiving step of receiving the decrypted E-mail transmitted in said transmission step to the client through said established Web encryption communication.

Claim 27 (Currently amended): A computer executable control program of a communication system including a server for providing a Web E-mail service to a client, said program comprising a management step of managing a key for decrypting an encrypted E-mail, a web encryption communication step for establishing a Web encryption communication with the client, and communicating with the client by the established Web encryption communication, an authentication step of executing authentication of the use allowance of the managed key to said client when said client requests to decrypt the encrypted E-mail while said server communicates with the client by said established Web encryption communication, a decrypting step of decrypting the encrypted E-mail using the managed key in the case where the use allowance is authenticated in said authentication step, and a transmission control step of

controlling to transmit the E-mail decrypted in said decrypting step to said client through said established Web encryption communication.

Claim 28 (Currently amended): A control program of a communication system including a client receiving a Web E-mail service through a Web from a server, comprising a step of executing a management step of managing a key for decrypting an encrypted E-mail, a web encryption communication step for establishing a Web encryption communication with the client, and communicating with the client by the established Web encryption communication, an authentication step of executing authentication of the use allowance of the managed key to said client based on authentication information sent from said client when said client requests to decrypt the encrypted E-mail while said server communicates with the client by the established Web encryption communication, a decrypting step of decrypting the encrypted E-mail using the managed key in the case where the use allowance is authenticated in said authentication step, and a transmission step of controlling to transmit the E-mail decrypted in said decrypting step to said client ~~in the server~~ through the established Web encryption communication, and said client comprising a requesting step of requesting to decrypt the encrypted E-mail while said Web encryption communication is established between the server and the client, an authentication information sending step of sending the authentication information for authentication in said authentication step, and a receiving step of receiving the decrypted E-mail transmitted in said transmission step to the client through said established Web encryption communication.

Claim 29 (Currently Amended): A storage medium storing a computer executable control program of a communication system including a server of providing a Web E-mail service to a client, the program comprising a step of executing a management step of managing a key for

decrypting said encrypted E-mail using said managed key, a web encryption communication step of establishing a Web encryption communication with the client, and communicating with the client by the established Web encryption communication, an authentication step of executing authentication of the use allowance of the managed key to said client when said client requests to decrypt the encrypted E-mail while said server communicates with the client by said established Web encryption communication, and a transmission control step of controlling to transmit the decrypted E-mail to said client ~~in a server~~ through said established Web encryption communication.

Claim 30 (Currently amended): A storage medium storing a control program of a communication system including a client receiving a Web E-mail service through a Web from a server, wherein the program comprises a step of executing a management step of managing a key for decrypting an encrypted E-mail, a web encryption communication step of establishing a Web encryption communication with the client, and communicating with the client by the established Web encryption communication, an authentication step of executing authentication of the use allowance of the managed key to said client based on authentication information sent from said client when said client requests to decrypt the encrypted E-mail while said server communicates with the client by said established Web encryption communication, a decrypting step of decrypting the encrypted E-mail using the managed key in the server in the case where the use allowance is authenticated in said authentication step, and a transmission control step of controlling to transmit the E-mail decrypted in said decrypting step to said client through the established Web encryption communication, the client comprising a requesting step of requesting to decrypt the encrypted E-mail while said Web encryption communication is established between the server and the client, an authentication information sending step of

sending the authentication information for authentication in said authentication step, and a receiving step of receiving the decrypted E-mail transmitted in said transmission step to the client through said established Web encryption communication.